Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра информационных технологий и систем безопасности

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Основная профессиональная образовательная программа
высшего образования по направлению подготовки

42.03.01 – Реклама и связи с общественностью

Направленность (профиль): **Реклама и связи с общественностью**

Квалификация:
Бакалавр

Форма обучения
Очная

Согласовано
Руководитель ОПОП
«Реклама и связи с общественностью»

_____**Фейлинг Т.Б.**

Утверждаю
Председатель УМС _____**И.И. Палкин**

Рекомендована решением
Учебно-методического совета
11 06 2019 г., протокол № 7

Рассмотрена и утверждена на заседании кафедры
21 05 2019 г., протокол № 10
Зав. кафедрой_____**Татарникова Т.М.**

Автор-разработчик:
_____ **Татарникова Т.М.**

Санкт-Петербург 2019

1. Цель и задачи освоения дисциплины «Информационная безопасность и защита информации»

Цель освоения дисциплины: формирование у студентов комплекса знаний, навыков и компетенций в области информационной безопасности и применения на практике методов и средств защиты информации.

Основные задачи дисциплины:

– Сформировать у студентов знания о современных тенденциях угроз информационной безопасности, о нормативных правовых документах по защите информации;

– сформировать у студентов устойчивое понимание роли и значения информационной безопасности личности, общества и государства и информационной инфраструктуры общества и государства;

– сформировать у студентов общие представления о современных методах и средствах защиты информации.

2. Место дисциплины в структуре основной образовательной программы

Дисциплина «Информационная безопасность и защита информации» относится к базовой части ОПОП, обеспечивающей подготовку бакалавров по направлению 42.03.01 «Реклама и связи с общественностью»

Дисциплина изучается во 2 семестре, объем дисциплины –144 ак. часа, 4 з.е.

Параллельно с данной дисциплиной изучаются социально-экономические дисциплины, которые формируют общие представления о системе профессиональной деятельности и социальных ценностях.

Для освоения учебной дисциплины, студенты должны:

− ***знать*****:** основные задачи информационной безопасности, методы и средства и технологии их решения;

− ***уметь*****:** логически верно, аргументировано и ясно строить устную и письменную речь; организовать свой труд; оценить защищенность и обеспечение информационной безопасности объектов информатизации;

− ***владеть*****:** навыками самостоятельной, творческой работы; способностью использовать для решения задач обеспечения информационной безопасности современные технические средства и информационные технологии.

Основными видами занятий при изучении дисциплины являются лекции и практические занятия. На лекциях излагаются наиболее сложные вопросы, имеющие концептуальное и методологическое значение в решении задач обеспечения информационной безопасности.

На практических занятиях отрабатываются ключевые практические вопросы, формируются необходимые умения и навыки защиты информации.

3. Перечень планируемых результатов обучения

Процесс изучения дисциплины направлен на формирование компетенций:

Универсальная компетенция

Категория общепрофессионльных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
Разработка и реализация проектов	**УК-2** Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**ИД-1$_{УК-2.}$** Формулирует в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Определяет ожидаемые результаты решения выделенных задач. **ИД-2$_{УК-2.}$** Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений. **ИД-3$_{УК-2.}$** Решает конкретные задачи проекта заявленного качества и за установленное время. **ИД-4$_{УК-2.}$** Публично представляет результаты решения конкретной задачи проекта.

Общепрофессиональная компетенция

Категория общепрофессионльных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
Аудитория	**ОПК-4** Способен отвечать на запросы и потребности общества и аудитории в профессиональной деятельности	**ИД-1$_{ОПК-4.}$** Соотносит социологические данные с запросами и потребностями общества и отдельных аудиторных групп. **ИД-2$_{ОПК-4.}$** Использует основные инструменты поиска информации о текущих запросах и потребностях целевых аудиторий / групп общественности, учитывает основные характеристики целевой аудитории при создании текстов рекламы и связей с общественностью и (или) иных коммуникационных продуктов.

Профессиональная компетенция

Задача ПД	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ опыта)
Тип задач профессиональной деятельности: организационный				
Участие в проектировании программ и отдельных мероприятий в области рекламы и связей с общественностью; организация работ по созданию и редактированию контента сайта.	Корпоративные и глобальные коммуникации, имидж компании, бренд компании (товарная марка, личный бренд), продукт рекламы, средства рекламы, включая печатные издания, телевизионные и радиопрограммы, сетевые издания, информационные ресурсы в сети Интернет.	**ПК-4** Способен организовать профессиональные мероприятия, направленные на формирование репутационного образа компании (продукта, персоны, др.) и сбыт продукции	**ИД-1$_{ПК-4.}$** Применяет знания организации профессиональных мероприятий, направленных на формирование репутационного образа компании (продукта, персоны, др.) и сбыта продукции. **ИД-2$_{ПК-4.}$** Участвует в мероприятиях, направленных на сбыт продукции и формирование репутационного образа компании (продукта, персоны, др.) **ИД-3$_{ПК-4.}$** Осуществляет контроль и оценивает эффективность мероприятий направленных на формирование репутационного образа компании (продукта, персоны, др.) и сбыт продукции	ПС. 06.009 Специалист по продвижению и распространению продукции средств массовой информации ПС.06.013 Специалист по информационным ресурсам

4. Структура и содержание дисциплины

Общий объем дисциплины составляет 144 ак. часов, 4 з.е.

4.1.Объем дисциплины (модуля) по видам учебных занятий (в академических часах)

набор 2019 г

Объём дисциплины	Всего часов
	Очная форма обучения
Общая трудоёмкость дисциплины	**144**
Контактная работа обучающихся с преподавателям (по видам аудиторных учебных занятий) – всего:	**56**
в том числе:	
лекции	**28**
практические занятия	**28**
Самостоятельная работа (СРС) – всего:	**88**
в том числе:	
курсовая работа	**-**
контрольная работа	**-**
Вид промежуточной аттестации	**Экзамен**

4.2. Структура дисциплины

Раздел	Раздел и тема дисциплины	Семестр	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля успеваемости	Занятия в активной и интерактивной форме, час.	Формируемые компетенции
			Лекции	Семинар.	Сам. работа			
Раздел 1. Основы информационной безопасности	Тема 1.1. Основные понятия и определения.	**2**	**2**	**2**	**6**	Дискуссия, обсуждение актуальных вопросов темы.	2	**ИД-2$_{ОПК-4.}$ ИД-1$_{ПК-4.}$**
	Тема 1.2. Задачи информационной безопасности.	**2**	**2**	**4**	**8**	Обсуждение актуальных вопросов темы, дискуссии.	4	**ИД-1$_{УК-2.}$ ИД-3$_{ПК-4.}$ ИД-2$_{ПК-4.}$**
	Тема 1.3. Угрозы информационной безопасности.	**2**	**2**	**2**	**8**	Обсуждение актуальных вопросов темы, решение заданий, дискуссии	2	**ИД-3$_{УК-2.}$ ИД-1$_{ПК-4.}$ ИД-3$_{ПК-4.}$**
	Тема 1.4. Основы госу-	**2**	**2**	**4**	**10**	Обсуждение	4	**ИД-1$_{ОПК-4.}$**

	дарственной политики и угрозы безопасности Российской Федерации в информационной сфере.					актуальных вопросов темы, решение заданий, дискуссии		**ИД-3$_{ПК-4.}$**
	Тема 1.5. Понятие и виды защищаемой информации.	**2**	**2**	**2**	**6**	Обсуждение актуальных вопросов темы, решение заданий, дискуссии	2	**ИД-1$_{ОПК-4.}$ ИД-2$_{ОПК-4.}$**
Раздел 2. Защита информации	Тема 2.1. Общая характеристика способов и средств защиты информации.	**2**	**2**	**2**	**10**	Обсуждение актуальных вопросов темы, решение заданий, дискуссии	2	**ИД-1$_{УК-2.}$ ИД-2$_{УК-2.}$ ИД-3$_{ПК-4.}$ ИД-4$_{ПК-4.}$**
	Тема 2.2. Криптографические методы защиты информации	**2**	**4**	**4**	**12**	Решение ситуационных задач, решение заданий	4	**ИД-4$_{ПК-4.}$ ИД-2$_{УК-2.}$**
	Тема 2.3. Методы организации безопасного доступа	**2**	**4**	**4**	**10**	Решение заданий	4	**ИД-2$_{УК-2.}$ ИД-1$_{ПК-4.}$ ИД-3$_{ПК-4.}$ ИД-4$_{ПК-4.}$**
	Тема 2.4. Электронная цифровая подпись и цифровые сертификаты	**2**	**4**	**2**	**8**	Решение заданий.	4	**ИД-2$_{УК-2.}$ ИД-1$_{ПК-4.}$ ИД-3$_{ПК-4.}$ ИД-4$_{ПК-4.}$**
	Тема 2.5. Программно-аппаратные средства защиты информации.	**2**	**2**	**2**	**8**	Обсуждение актуальных вопросов темы, он-ные/творческие задачи	2	**ИД-2$_{УК-2.}$ ИД-1$_{ПК-4.}$**
	ИТОГО		**28**	**28**	**88**	**Экзамен**	**28**	

4.3. Содержание дисциплины

Раздел 1. Основы информационной безопасности

Тема 1.1. Основные понятия и определения.

Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности. Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженерно-техническая защита информации. Криптографическая защита информации. Представление информации в цифровом виде.

Тема 1.2. Задачи информационной безопасности.

Задача обеспечения конфиденциальности. Задача обеспечения аутентификации. Обеспечение идентификации. Задача обеспечения целостности.

Тема 1.3. Угрозы информационной безопасности.

Классификация угроз информационной безопасности. Угрозы несанкционированного доступа к данным. Угрозы нарушения целостности данных. Угрозы нарушения конфиденциальности данных.

Тема 1.4. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.

Основы законодательства в области обеспечения информационной безопасности. Правовое обеспечение информационной безопасности.

Российское законодательство в области информационной безопасности. Закон "Об информации, информатизации и защите информации". Другие законы и нормативные акты.

Тема 1.5. Понятие и виды защищаемой информации

Путь конфиденциального документа от создания до уничтожения: решение, разработка проекта, подготовка содержания, реквизитов, передача, получение, исполнение и архивация. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Защита конфиденциальной информации при ее передаче по сети.

Система защищенного электронного документооборота.

Раздел 2. Защита информации

Тема 2.1. Общая характеристика способов и средств защиты информации.

Способы и средства защиты информации от несанкционированного доступа.

Способы и средства защиты информации от вредоносного кода.

Способы и средства защиты информации от межсетевого воздействия.

Способы и средства криптографической защиты информации.

Тема 2.2. Криптографические методы защиты информации

Основные понятия криптографии. Симметричные шифры. Криптография с открытым ключом.

Тема 2.3. Методы организации безопасного доступа

Схемы идентификации и аутентификации. Одно- и многофакторная аутентификация. Система разграничения доступа к информации в компьютерной системе. Концепция построения систем разграничения доступа.

Средства и методы ограничения доступа к файлам.

Тема 2.4. Электронная цифровая подпись и цифровые сертификаты

Понятие о цифровой подписи. Подпись RSA. Подпись ElGamal. Подпись DSA. ЭЦП ГОСТ Р 34.10-94 и ГОСТ Р 34.10-01.

Инфраструктура открытых ключей. Сертификаты открытых ключей.

Тема 2.5. Программно-аппаратные средства защиты информации
Аппаратные и программно-аппаратные средства криптозащиты данных. Использование дополнительных плат расширения. Методы “водяных знаков” и методы “отпечатков пальцев”. Защита программ от несанкционированного копирования. Вирусы.

4.4. Семинарские, практические, занятия, их содержание

№ темы дисциплины	Тематика практических занятий	Форма проведения	Формируемые компетенции
Тема 1.1	Классификации видов, методов и средств защиты информации.	Дискуссия, обсуждение актуальных вопросов темы.	**ИД-2$_{ОПК-4.}$ ИД-1$_{ПК-4.}$**
Тема 1.2.	Задачи информационной безопасности.	Обсуждение актуальных вопросов темы, дискуссии.	**ИД-1$_{УК-2.}$ ИД-3$_{ПК-4.}$ ИД-2$_{ПК-4.}$**
Тема 1.3.	Практикум: угрозы информационной безопасности. Вирусы.	Обсуждение актуальных вопросов темы, решение заданий, дискуссии	**ИД-3$_{УК-2.}$ ИД-1$_{ПК-4.}$ ИД-3$_{ПК-4.}$**
Тема 1.4.	Практикум: сбор информации о деятельности организации.	Обсуждение актуальных вопросов темы, решение заданий, дискуссии	**ИД-1$_{ОПК-4.}$ ИД-3$_{ПК-4.}$**
Тема 1.5.	Практикум: Настройка локальных политик безопасности автоматизированного рабочего места	Обсуждение актуальных вопросов темы, решение заданий, дискуссии	**ИД-1$_{ОПК-4.}$ ИД-2$_{ОПК-4.}$**
Тема 2.1.	Основные способы и средства защиты информации: сравнительная характеристика	Обсуждение актуальных вопросов темы, дискуссии	**ИД-1$_{УК-2.}$ ИД-2$_{УК-2.}$ ИД-3$_{ПК-4.}$ ИД-4$_{ПК-4.}$**
Тема 2.2.	Практикум: алгоритмы шифрования данных	Решение ситуационных задач, решение заданий	**ИД-4$_{ПК-4.}$ ИД-2$_{УК-2.}$**
Тема 2.3.	Практикум: биометрические системы	Решение заданий	**ИД-2$_{УК-2.}$ ИД-1$_{ПК-4.}$ ИД-3$_{ПК-4.}$ ИД-4$_{ПК-4.}$**
Тема 2.4.	Практикум: алгоритмы электронной цифровой подписи	Решение заданий.	**ИД-2$_{УК-2.}$ ИД-1$_{ПК-4.}$ ИД-3$_{ПК-4.}$ ИД-4$_{ПК-4.}$**
Тема 2.5.	Методы “водяных знаков” при решении авторского права.	Обсуждение актуальных вопросов темы, ситуационные/творческие задачи	**ИД-2$_{УК-2.}$ ИД-1$_{ПК-4.}$**

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для эффективного освоения курса дисциплины и сформированности заявленных компетенций темы дисциплины сопровождаются методическими материалами:

методические указания по выполнению самостоятельной работы (в электронном виде на кафедре ИТУвГСБ);

примеры выполнения заданий (доступ moodle.rshu).

6. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Предусмотрены следующие виды контроля и аттестации обучающихся при освоении дисциплины:

Для оценивания результатов обучения в виде знаний используются:

− индивидуальное собеседование, дискуссия;

Для оценивания результатов обучения в виде умений и владений используются следующие типы контроля:

− решение заданий;

− творческие задачи.

Фонды оценочных средств, включающие типовые задания и методы оценки, критерии оценивания позволяющие оценить результаты освоения данной дисциплины, входят в состав РПД на правах отдельного документа.

6.1. Текущий контроль

Типовые задания, методика выполнения и критерии оценивания текущего контроля по разделам дисциплины представлены в Фонде оценочных средств по данной дисциплине. Фонды оценочных средств входят в состав РПД на правах отдельного документа.

6.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине проводится в форме устного экзамена по темам курса.

Примеры дискуссионных тем.

1. Ценность информации. Цена информации.
2. Мероприятия по управлению доступом к информации.
3. Методы несанкционированного доступа к информации.
4. Процедура идентификации, как основа процесса обнаружения объекта.
6. Защита личности как носителя информации.
7. Классификация вирусов.
8. Компьютерная преступность. Виды преступной деятельности.
9. Классификация антивирусных программ.
10. Этапы разработки мер по предотвращению угроз утечки информации.

Примеры заданий

Приведите процедуру аутентификации пользователя со следующими исходными данными: имя пользователя (*Name*), пароль (*Password*), случайное число (*V*). Процедура перемешивания состоит в последовательном перемешивании полубайтов пароля и случайного числа. Вычисление дайджеста состоит в вычислении остатка перемешенного числа по модулю *Password.*

Примерные вопросы для промежуточной аттестации по дисциплине

1. Определение информационной безопасности.
2. Критические данные.
3. Признаки компьютерных преступлений в интернет технологиях.
4. Основные технологии и методы компьютерных преступлений.
5. Уровня защиты компьютерных (интернет технологий) и информационных ресурсов.
6. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
7. Концепция обеспечения безопасности информационных систем.
8. Избирательная политика управления доступом.
9. Организационные меры безопасности информационных систем.
10. Матрица доступа в АСОИ.
11. Полномочное управление доступом.
12. Избирательное управление доступом.
13. Оценочные стандарты и технические спецификации.
14. Угрозы безопасности данных
15. Источники нарушений безопасности
16. Аутентификация
17. Авторизация пользователей
18. Методы парольной аутентификации. Недостатки методов аутентификации с запоминаемым паролем.
19. Аутентификация с помощью биометрических характеристик.
20. Принципы работы биометрических систем.
21. Реализация биометрических систем.
22. Поведенческие биометрические характеристики.
23. Атаки на биометрические системы.
24. Концепция шифрования на открытом ключе.
25. Концепция шифрования на закрытом ключе
26. Понятие хэш-функции. Общая схема образования хэш-функции.
27. ЭЦП RSA
28. ЭЦП Эль-Гамаль
29. ЭЦП ГОСТ Р 34.10-2001
30. Базовая модель криптографии.

7. Методические указания для обучающихся по освоению дисциплины

Методические рекомендации по работе во время лекционных занятий

В ходе лекционных занятий рекомендуется конспектировать учебный материал, представляемый преподавателем. Общие и утвердившиеся в практике правила, и приемы конспектирования лекций:

1.Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

2.Необходимо записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

3.Ссылки на первоисточники отмечать на полях, чтобы при самостоятельной работе найти и вписать их в текст конспекта.

4.В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

5.Каждому студенту необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

6.В конспект следует заносить всё, что преподаватель пишет на доске, а также рекомендуемые схемы, таблицы, диаграммы и т.д.

Методические рекомендации по подготовке к практическим занятиям

Целью практических занятий является углубление и закрепление теоретических знаний, полученных студентами на лекциях и в процессе самостоятельного изучения учебного материала, формирование у них определенных умений и навыков, формирование части компетенции.

В ходе подготовки к практическому занятию необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить практические задания. При этом учесть рекомендации преподавателя и требования программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы. Желательно при подготовке к практическим занятиям по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.

Подготовка к зачёту/экзамену.При подготовке к промежуточной аттестации необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и выполнение заданий на практических занятиях.

8. Учебно-методическое и информационное обеспечение дисциплины

а) *Основная литература:*

1. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-00091-007-8. Режим доступа: http://znanium.com/catalog/product/491597

2. Бабаш А.В. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В. - 3-е изд. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.: 60x90 1/16. - (Высшее образование) (Пе-

реплёт) ISBN 978-5-369-01450-9 - Режим доступа: http://znanium.com/catalog/product/495249.

3. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. - 2-е изд., перераб. и доп. - Москва: ДМК Пресс, 2017. - 434 с. ISBN 978-5-97060-435-9. Текст: электронный. URL: http://znanium.com/catalog/product/1028060.

б) *Дополнительная литература:*

1. Защищенные корпоративные сети. Раздел: «Задачи по защите информации» [Текст]: учебное пособие / Т. М. Татарникова; РГГМУ. Санкт-Петербург: РГГМУ, 2012. – 113 с.

2. Криптографические методы защиты информации [Текст]: лабораторный практикум / Т. М. Татарникова; РГГМУ. Санкт-Петербург: РГГМУ, 2013. – 63 с.

3. Криптографические методы защиты информации. [Текст]: методические указания к выполнению лабораторных работ / Т. М. Татарникова; РГГМУ. Санкт-Петербург: РГГМУ, 2010. – 50 с.

в) *Программное обеспечение и Интернет-ресурсы*:

1. Windows 7 48130165 21.02.2011
   Office 2010 49671955 01.02.2012
2. Электронная библиотека ЭБС: «Znanium» (http://znanium.com/), ЮРАЙТ
3. Интернет-ресурсы: https://210fz.ru/fz-ob-informacionnoj-bezopasnosti/ - законы РФ по информационной безопасности

9. Материально-техническое обеспечение дисциплины

Учебная аудитории для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования.

Учебная аудитории для проведения занятий семинарского типа - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Учебная аудитория для групповых и индивидуальных консультаций - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Учебная аудитория для текущего контроля и промежуточной аттестации - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Аудитория для самостоятельной работы - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

10. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов,

составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.